Trust-Based Decision Making for Environmental Health Community of Interest IoT Systems

Hamid Al-Hamadi[†] and Ing-Ray Chen[*]

[†]Department of Computer Science
Kuwait University
hamid@cs.ku.edu.kw

[*]Department of Computer Science
Virginia Tech
irchen@vt.edu

Abstract—**With the onset of the Internet of Things (IoT) era, the number of devices and sensors is increasing tremendously. This paper is concerned with Health IoT consisting of various devices carried by members of an environmental health community of interest (CoI). We propose trust based information sharing among the CoI users of these IoT devices, so that a collective knowledge base can be built to rate the environment at a particular location and at a given time. This rated knowledge of various environments would enable a user's mobile device to automatically decide whether or not the user should visit this place/environment. Our trust-based decision making framework considers risk classification, reliability trust, and loss of health probability as three design dimensions for decision making. Performance data are shown to demonstrate the feasibility of our approach.**

Keywords—**Internet of things, community of interest, trust management, risk, health decisions, health IoT.**

I. INTRODUCTION

In this paper, we propose a trust-based approach for information sharing in an environmental health community of interest (CoI) Internet of Things (IoT) system. Members of the CoI share the location-based information obtained through their personal area networks (PANs) with the goal of maximizing the safety of each member. Through the use of trust management, our system guides members of the CoI to use the most trustworthy information to make decisions on environmental health and in particular whether or not to enter a location at a particular time.

Bloomberg news [1] reported that internet of things would be 19 trillion dollar market in next few years. Before the majority of us could realize, these devices have already become available for day to day activities and are available in commercial market. Such devices [2] [3] available at a very affordable price, when combined with mobile phones, can provide high quality readings for various environmental parameters, like CO levels, humidity, hydrocarbons, particulate matter, dust and so on. As more and more people start using these devices, the cost is expected to come down sharply. Thereby further giving a push to the usage of these devices in everyday life. Once these devices become so popular in near future, so many interesting scenarios are expected to appear. Since the measurement of environment has a direct relation with the healthcare of certain ailments, and health in general, these devices are expected to play a major role in providing excellent support in day-to-day healthcare. For example an elderly person suffering with high blood pressure might not want to go to a place where noise levels are very high. Since these physical attributes of the environment can directly be measured by the common devices already available in market, we expect that such a use would become more common in near future. Prior knowledge of the environment can guide safe decision making.

The knowledge of the health IoT is gained through the collaboration of the many user devices, which enable information collection of a wide range of parameters like noise, chemical fumes, fragrances, and so on. In fact some such ratings of cities have already started to come up on different websites [4].

Also, it is difficult for health professionals to personally attend to all patients at all times. It is even more difficult to give personalized assessments regarding the health risk for patients entering into different physical locations due to the absence of monitoring tools providing detailed location-aware information which spans large, geographic areas. Furthermore, any health decision should also take into account the current health status of a patient.

This paper describes a trust-based approach in a health CoI-based IoT, with the goal of collecting trustworthy environmental health information and achieving reliable decision making. Members of the IoT rely on their devices for information sharing and decision making. In this work we are mainly concerned with providing a framework to suggest to the member whether or not it is safe for the member to visit a particular place. All these decisions are made solely by devices communicating with each other in a trust based co-operative network. We believe that such a system would be immensely helpful in improving the quality of life, without any overtly expenditure of effort on users' part. The system is resilient to small errors made in reading environment parameters. Even if a few users do not have some particular sensors (e.g. noise), the cooperation among the framework participants ensures good quality data to everybody in the health CoI.

II. Related Work

Many research papers are available on the security aspect of IoT systems. For example, in [5], the authors have discussed the need of adaptive security management and initial solutions for E-health IoT applications, for the treatment of chronic diseases and well-being of elderly people. Their paper discusses adaptive security management for setting the security requirements for enforcing the adequate security controls. In [6] the authors also discussed the security aspect of the IoT primarily through the means of authentication and authorization. Similarly [7] gave a detailed system of health IoT and then describes a privacy and security mechanism using the encryption technology. Our work is different is that we use trust to enhance security and to help users make decisions based on trust information.

In [8], the authors advocated the use of Internet to provide scalable and flexible architecture. They used RFID based devices which communicate over Internet to achieve a sort of parallel architecture which is highly scalable. Similarly [9] and [10] discussed security challenges in health IoT. Similarly, [11] discusses about the concept of Internet of m-health Things (m-IoT). This paper elaborates the use of 6LoWPAN technology in the devices to build a practical m-IoT of health. [8-11] cited above again only focused on security aspects of IoT. Our work considers trust-based mechanisms, allowing users to filter out untrustworthy input when gathering health information to enhance security.

The survey paper in [12] gives a very detailed analysis of contemporary trust management techniques in IoT. It however does not discuss the specific goals of health IoT. This paper nevertheless describes a novel approach towards health IoT in public domain, utilizing trust based mechanisms to achieve a reliable system. The novelty is in the use of trust management to effectively collect various geo-based health related data and to use this data for reliable decision making.

In [13] Josang et al. discussed the concepts of reliability trust and decision trust. The reliability trust corresponds to reputation/trust, while the decision trust involves reliability trust, cost and payoff as the key components for decision making. We will apply the concept of decision trust in this work for trust management of health CoI IoT. [14, 15] discussed trust management for web services and delay tolerant networks, respectively. While the trust management mechanisms proposed in [14, 15] for web services and delay tolerant networks are valid, they cannot be applied to health CoI IoT systems since the main characteristics of health IoT are not taken into consideration. Very recently [19-21] discussed trust management for social IoT systems. However, the emphasis is how the social relationship of distributed IoT entities would affect the trust relationships and thus the service dispositions between IoT devices which provide services toward each other.

Our work differs from the IoT trust works cited above in that we aim to achieve effective and scalable trust-based decision making to health CoI IoT members. We propose to leverage ubiquitous cloud service to serve a large number of mobile CoI IoT devices for scalability and to derive trust ratings from various sources to produce a system that is inherently reliable. The system has been designed in a way so that it promotes sharing of trustable data among CoI IoT members. The goal of the health CoI is to provide its members the most trustworthy information to make decisions resulting in the most reliable outcome with regards to their health. Members of the health CoI share their location-based information from their personal sensors. Thus the CoI is dependent on the collaboration of members and their devices. We consider the use of trust management to determine the most trustworthy data to be used by querying members for decision making.

III. System Model

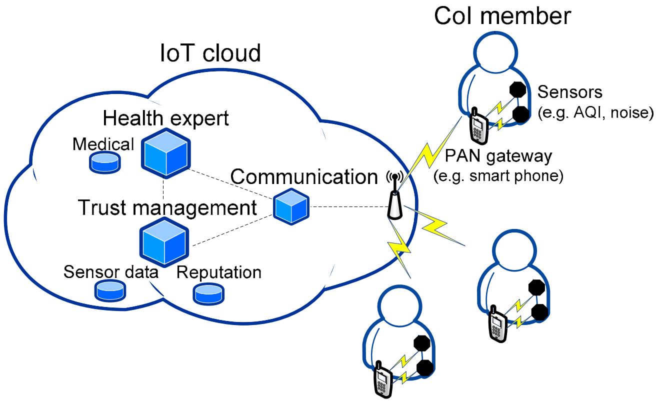

Figure 1: System Design of the Health CoI IoT.

In this section we describe the system design of the Health CoI IoT. Each member of the health CoI is equipped with a PAN consisting of a gateway device, and several sensors. For example, a smart phone can act as a gateway, and the sensors can be small devices possibly attached to the member's body or vehicle (e.g. wheelchair). These sensors act as IoT devices. Some of these sensors measure environment factors (e.g. Air Quality Index, noise, NO_2, CO, hydrocarbons, electromagnetic radiation and so on), while others measure personal health statistics. The measurements from personal health statistics would be used primarily to derive the risk that the user can take at a particular point in time, e.g., body temperature, rate of breathing, blood pressure and so on.

Environment data is shared among all users of the Health CoI while personal data related to the member is not shared and is used as input into the decision making process later on. By contributing to the CoI and sharing correct environment data, members make sure that they maximize their probability of correct decision making. Furthermore, members that misbehave by sending incorrect data increase their probability of being evicted from the CoI.

Furthermore, while sensor data is automatically collected and shared, a member can still use sensor data received so far in order to further its interests. Moreover, faulty sensors can give incorrect readings, due to malfunction. Thus a responsibility of the trust management protocol is to overcome these challenges and provide the most trustworthy data that matches the actual environment for a given location, for accurate decision making.

Figure 1 shows the system design space of the Health CoI IoT. The subsystems interact to carry out the functions of the Health CoI IoT. Since the Health CoI cloud can be accessed by all IoT devices ubiquitously wherever they are, we will interchangeably refer to it as the Central Authority (CA).

When a patient intends to change his location, he sends a query to the CA asking about the safety of entering this location. The CA performs the risk calculation utilizing the trust management and the health expert subsystems and responds to the query.

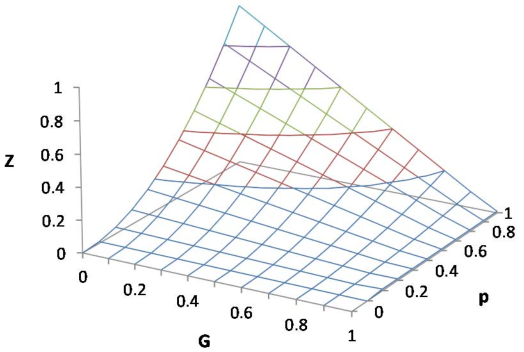

Figure 2: Parameter Z = (1-H) where H is the health classification by the doctor/medical center. Parameter p is the reliability trust of the source of the sensor data (environment parameters). Parameter G is the possibility of loss of health as derived from the sensor data.

Doctors evaluate the health of each member prior to joining the Health CoI (and periodically thereafter). Based on the health assessment evaluation, the healthiness level or fitness level, denoted by H, is assigned to each user of the system. A set of thresholds are defined by an expert medical system. This could be as simple as given a level of dust, a level of hydrocarbons in air or a temperature reading, which maps to a probability that the user suffering from particular disease might face worsening of health. Therefore, a graph is constructed as shown in Figure 2.

The above graph in Figure 2 depicts the decision plane concept. In the following, we provide a detailed description of each of the three parameters in the graph:

- A member's health classification by the Doctors (Z) – Doctors or medical team would analyze a person's medical record and would assign health level or fitness level parameter H. Then we calculate Z=1-H and plot this parameter Z. The scale of Z varies from 0 at the bottom to 1 at the top. In a way, we can define Z as the vulnerability index.
- Reliability trust of the source (p) – this parameter measures the trustworthiness of the agent who is providing the information.
- Probability of the loss of health (G) – This represents the possibility that the user might suffer worsening of his/her health as determined by the data sent by agent.

All the decision points below this graph are considered logically good decisions. Any of the decision points above this decision plane are considered risky decisions. For a very healthy person, H will be very high, say H = 0.9 (healthy); thus, Z=1-0.9=0.1. Now suppose, the trust on the agent/participant sending the sensor data is high, say p = 0.9. Also, the data sent by the agent can be mapped to a certain probability of worsening of user's health. Let this probability of loss of health (G) be 0.9. In this case this person can take this decision since the point would lie below the decision plane. But the person with Z=0.7 (not so healthy) cannot take this decision, because for him the point would lie above the decision plane. While the example suggests that G and p are from a single source, G and p can also be derived from multiple sources, through aggregation of G's and p's respectively.

The decision graph described above can be defined by an equation relating p with Z and G as follows: The higher the trust in the agent (who sends the data), the higher the Z value would be allowed. This is because the more one trusts the source of data and thereby the data itself, the more one can act on information even though one has a weaker health. The situation is opposite for G. The less the probability of harm to health, the more one can act on information, even though one might not be in best of health. Thus we define the following equation to relate p with Z and G.

$$Z = p^{\gamma} * (1 - G)^{\omega} \qquad (1)$$

Here γ and ω are tuning parameters. For this work we set γ =2 and ω =1 for illustration purposes.

In this paper we mainly consider the action to physically enter into an area. However, our model can be easily extended to other location based scenarios like evacuation of people from a building. A malicious member may show untrustworthy behavior to further its interests. For example, the member may send an incorrect rating (bad news) to the CA in order to minimize the contention with other members in that area. Furthermore, the member may be reluctant to waste its resources for the benefit of the CoI. In this paper we consider persistent attackers who aim to break down the CoI IoT. That is, a malicious attacker will always send incorrect readings about the measured phenomenon at a location to the CA. A malicious attacker may send a false location information to further disrupt the CoI IoT.

IV. Trust Management Protocol

In this section, we describe the trust management protocol for health CoI IoT. Table I lists the notation used in the paper.

A. Location Ratings

Each health CoI member can send the sensed data from its PAN to the CA. Let$R_{i,j}^{x}$ denote a rating (or report) sent from member i about location x regarding phenomenon j where $R_{i,j}^{x}$ is in the range of [0, 1]. Here we note that the phenomenon is measured by a particular sensor that is known to the IoT, and hence we will use j to denote the sensor or phenomenon measured by the sensor interchangeably. The CA receives the ratings sent from IoT members and stores them in the cloud.

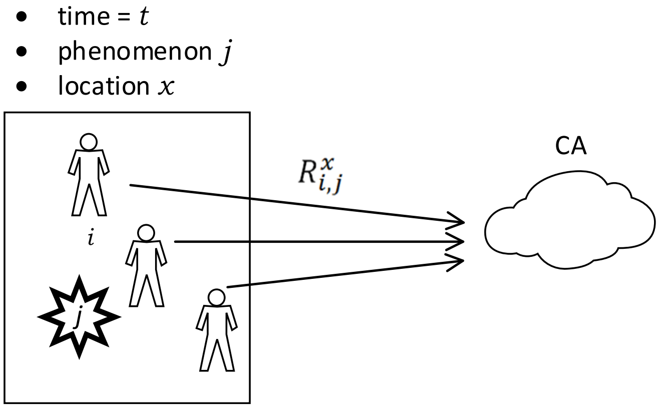

Figure 3: Member $\boldsymbol{i}$ sending location rating $\boldsymbol{R_{i,j}^{x}}$ at time $\boldsymbol{t}$ to the CA.

B. *Querying the CA*

Members obtain information regarding a particular location x by sending a query to the CA, denoted by $Q_{i,j}^{x}$, which represents a query from member i about location x regarding phenomenon j. The CA must examine its received reports about location x and form a query reply $QR_{i,j}^{x}$ to supply entity i with necessary information for decision making. One way is to derive both the aggregate rating for the location, and the associated trustworthiness for that aggregate rating. Let $WR_{i,j}^{x}$ denote the aggregated rating about location x regarding phenomenon j. We define $WR_{i,j}^{x}$ as follows:

$$WR_{i,j}^{x} = \frac{\sum_{k \in A_j^x} \partial \times C_{k,j} \times R_{k,j}^{x}}{\sum_{k \in A_j^x} \partial \times C_{k,j}} \tag{2}$$

where ∂ is a decay factor based on when $R_{k,j}^{x}$ was issued. The capability of the device used by member k to sense phenomenon j denoted by $C_{k,j}$ is expressed by a range between 0 and 1 where $C_{k,j}$ closer to 1 means that the device is more capable of capturing accurate readings for phenomenon j. The CA is responsible for inferring $C_{k,j}$.

The aggregated trust of rating intended for answering member i about location x regarding phenomenon j is:

$$TR_{i,j}^{x} = \frac{\sum_{k \in A_j^x} T_{k,j}^{x}}{\left|A_j^x\right|} \tag{3}$$

where $\left|A_j^x\right|$ is the total number of reports about phenomenon j in location $x$and $T_{k,j}^{x}$ (to be discussed later in Section IV.C) is the trust of member k about location x regarding phenomenon j. The CA can then use $(WR_{i,j}^{x}, TR_{i,j}^{x})$ for decision making. The parameter $WR_{i,j}^{x}$ can be used to derive G. A static table created (one time exercise) by the medical experts can map $WR_{i,j}^{x}$ to G in the decision graph. The parameter $TR_{i,j}^{x}$ corresponds to parameter p in the decision graph (shown in Figure 2), while $WR_{i,j}^{x}$ corresponds to parameter G in the graph. The CA then can make a decision whether the user should enter the location or not based on if the data point (Z, p, G) falls below or above the decision plane.

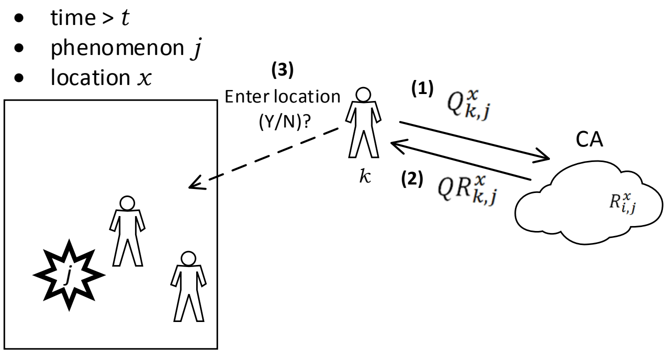

Figure 4: Steps for member decision making in the Health CoI IoT: (1) Member **j** querying CA, (2) CA replying with decision or decision making information, (3) Member **j** decides based on obtained information and risk model (and possible local assessment), whether to enter location **x**.

C. *CoI Member Trust*

There is a trust score associated with each CoI member indicating how trustworthy that member is. A member's trust is time dependent, and more recent assessments of its trustworthiness rating contribute more to its current trust. The CA periodically calculates every member’s rating and subsequently updates the member’s trust. Let T_k be the trust score of member k as computed by the CA, and $RR_{k,I}$ be the trust rating given by the CA in the I^{th} period. We define T_k as follows:

$$T_k = \frac{\sum_{I=1}^{trc} \partial_I \times RR_{k,I}}{\sum_{I=1}^{trc} \partial_I} \tag{4}$$

where trc is the total number of periodic ratings that have been executed by the CA, and $\partial_I$is the decay factor for the rating computed in the I^{th} rating interval. Member k's rating at the I^{th} interval $RR_{k,I}$ can be derived as:

$$RR_{k,I} = \alpha\left(RR_{k,I}^{loc\_rating}\right) + \beta\left(RR_{k,I}^{rater}\right) + \gamma(RR_{k,I}^{loc\_verif}) \tag{5}$$

where α, β and γ (with $\alpha + \beta + \gamma = 1$) are weights to prioritize three different rating factors ($RR_{k,I}^{loc_rating}$for location rating, $RR_{k,I}^{rater}$ for rater rating, and $RR_{k,I}^{loc_verif}$for witness rating) that are assessed when computing a single trust rating. Below we discuss these rating factors.

$\boldsymbol{RR_{k,I}^{loc\_rating}}$: Every location rating given by a rater k is judged by the query issuer i after i actually enters location x. That way i can provide a feedback of whether k was malicious or fabricated. This also needs to take into account the trust of i, since it can in turn fabricate its feedback. Thus we have:

$$RR_{k,I}^{loc\_rating} = \frac{\sum_{j\in K_j}\sum_{x\in K_x}\sum_{i\in FS(R_{k,j}^{x})} T_i \times \partial_{afr} \times d(f_i(R_{k,j}^{x}), R_{k,j}^{x})}{\sum_{j\in K_j}\sum_{x\in K_x}\sum_{i\in FS(R_{k,j}^{x})} T_i \times \partial_{afr}} \quad (6)$$

where K_j is the set of all ratings reported by member k regarding phenomenon j, and $K_x$is the set of all ratings reported by member k regarding location x. $FS(R_{k,j}^{x})$ is the feedback set of all members who used the rating $R_{k,j}^{x}$ provided by member k, ∂_{afr} is a feedback factor parameter for taking into account the distance between time of assessment $t(RR_{k,i})$, time of feedback $t(f_i(R_{k,j}^{x}))$, and time of location rating $t(R_{k,j}^{x})$. Thus we have $\partial_{afr} = \lambda^{\sigma}$ where σ is the standard deviation of these three timings. $d(f_i(R_{k,j}^{x}), R_{k,j}^{x})$ represents the similarity between the two location phenomenon measurements, defined as:

$$d(f_i(R_{k,j}^{x}), R_{k,j}^{x}) = 1 - |f_i(R_{k,j}^{x}) - R_{k,j}^{x}| \quad (7)$$

The basic idea of Equation 7 is to effectively judge the phenomenon measurement that should have been there with what was actually seen once there by i (supposedly).

$\boldsymbol{RR_{k,I}^{rater}}$**:** In addition to judging location raters, we judge members by the accuracy of their feedback towards the location raters. A possible way to do that is to contrast the feedback rating with the majority of feedback ratings about the same phenomenon at that location. Let us assume that k gave feedback $f_k(R_{i,j}^{x})$ about location rating $R_{i,j}^{x}$ provided by member i, and that other feedback providers (each represented by u) gave their feedbacks about the same phenomenon. Then

$$RR_{k,I}^{rater} = \frac{\sum_{\substack{\forall i\, \forall x\, \forall u\in FS(R_{i,j}^{x}) \\ AND\ k\in FS(R_{i,j}^{x})}} T_u \times \partial_{aff} \times d(f_u(R_{i,j}^{x}), f_k(R_{i,j}^{x}))}{\sum_{\substack{\forall i\, \forall x\, \forall u\in FS(R_{i,j}^{x}) \\ AND\ k\in FS(R_{i,j}^{x})}} T_u \times \partial_{aff}} \quad (8)$$

where $\partial_{aff} = \lambda^{\sigma}$ and σ is the standard deviation of $t(RR_{k,i}), t(f_u(R_{i,j}^{x})), and\ t(f_k(R_{i,j}^{x})$.

$\boldsymbol{RR_{k,I}^{loc\_verif}}$: At every interval I, the CA examines the trustworthiness of its received ratings by all members since the last time interval. It relies on data from members that vouch for the correctness of the claim that another member was in fact in a location at a specific time. This can be verified since they were able to communicate over short range transmission (works as a substitution for physical eye sight) and this can be relayed (piggybacked) back to the CA periodically. The benefit is twofold. First, Members that have been seen by other members in the reported location gain trust. Second, It can detect misbehavior in reported location ratings, which includes a member sending a rating from two distant locations at the same time, or a member claiming to be at a location, but seen elsewhere. Let $OS_{k,t}^{x1}$ be the set of members that have come in contact with member k at time t at location $x1$ when k sent rating $R_{k,j}^{x2}$ to CA (each represented by i). For each member i, If $x1 = x2$ then i agrees that k was at the claimed location at time t and hence the CA sets the weight for location verification to $w_i = 1$ to increase its trust. Otherwise if $x1 \neq x2$, then $k's$ location rating is considered suspicious based on information supplied by i, and so CA sets $w_i = 0$. This is done for every i that has claimed to be in the vicinity of k at time t. In case there is no observation for or against i, the CA sets $RR_{k,i}^{loc\_verif}$ to a neutral value of 0.5. Thus we have:

$$RR_{k,I}^{loc\_verif} = \begin{cases} \dfrac{\sum_{i\in OS_{k,t}^{x1}} T_i \times w_i}{\sum_{i\in OS_{k,t}^{x1}} T_i}, & |i \in OS_{k,t}^{x1}| \neq \emptyset \\ 0.5\,, & |i \in OS_{k,t}^{x1}| = \emptyset \end{cases} \quad (9)$$

V. Performance Evaluation

TABLE I: Parameters.

Name	Value	Name	Value
$M \times M$	10×10(1km×1km)	S_{ph}	0.2m/s
N_T	100	T_{period}	1hr
P_m	$[0, 30\%]$	T	20hrs
S_N	1m/s		

In this section we perform ns3 simulation for performance evaluation of our trust-based decision making framework. Our performance metric is the correct decision ratio (CDR), i.e., the ratio of the number of correct decisions over the total number of decisions, by a user. This performance metric is measured dynamically. As more information is collected regarding the trustworthy behavior of nodes in the system, more correct decisions are made and CDR should converge to a high value as time progresses. Table I lists the parameters used in the simulation. In our experimental setup we consider an environmental health CoI with N_T=100 members each using one smart IoT device for simplicity. The percentage of malicious nodes is specified by a parameter $P_m \in [0, 30\%]$ to test the effect of malicious population on performance. The malicious nodes are randomly selected out of all IoT devices. A node selected to be in this "malicious" population remains malicious throughout the simulation. All nodes move randomly in an M-cell by M-cell operational area. A hazardous condition is created and is moving albeit at a slower speed (0.2m/s) than the average node mobility (1m/s). A node issues a query before it steps into a cell and based on the cloud server's recommendation decides to enter the cell or not. The mobility route changes if the recommendation is no. The CA calculates the trust scores of the members every T_{period} = 1hr, and the total simulation time is T=20 hours so we can observe the CDR convergence behavior. We set the trust rating factor weights to $\alpha = \beta = \gamma = 1/3$.

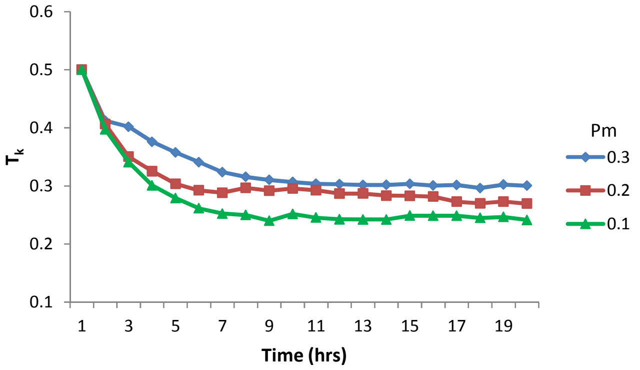

Figure 5: $\boldsymbol{T_k}$ vs. time for a randomly selected malicious node *k*.

Figure 5 shows $T_k$vs. time for a malicious node k randomly selected. We see that as time progresses, the trust score of this malicious node decreases and finally converges to a low value. This demonstrates the effectiveness of our designed mechanisms against malicious attacks.

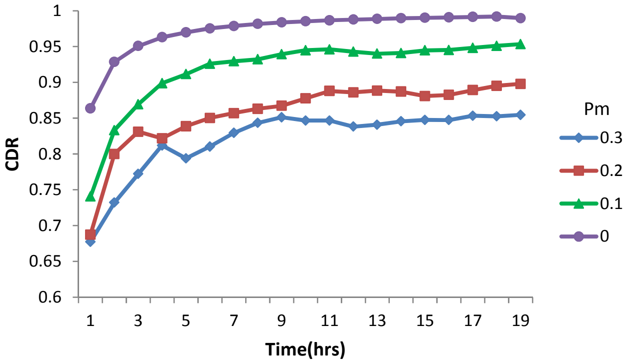

Figure 6: CDR vs. time for a good node randomly selected over a range of $\boldsymbol{P_m} \in [\mathbf{0}, \mathbf{30}\%]$

Figure 6 shows CDR vs. time for a good node randomly selected over a range of $P_m \in [0, 30\%]$ in increment of 10%. We see that when there is no malicious node in the system, CDR converges fairly quickly as more information is collected as time progresses. The convergence time increases as $P_m$increases. However, we see that CDR eventually converges to a high value even when $P_m$is as high as 30%. We attribute this to the ability of our trust protocol to discern malicious nodes from good nodes and the effectiveness of our trust-based decision making framework to make correct decisions based on the relationship between the patient's risk classification, the decision's reliability trust, and the decision's loss of health probability.

VI. Conclusion

In this paper we proposed and analyzed a trust-based risk management framework for environmental health community of interest IoT systems. We described the problem and thus the motivation to create a trust-based decision making framework for health CoI IoT. Our trust-based decision making framework considers risk classification, reliability trust, and loss of health probability as three design dimensions for decision making. We developed a trust protocol for environmental health CoI IoT to assess the reliability trust of individual IoT devices which supply sensing reports, as well as the loss of health probability should the user enter a given location at a given time. Our simulation results demonstrated the feasibility of our approach with a high correct decision ratio.

Acknowledgment

This work was supported and funded by Kuwait University Research Grant #QS01/15.

References

[1] Bloomberg, "Cisco CEO Pegs Internet of Things as $19 Trillion Market," *Bloomberg news,* 2014.

[2] http://www.sensorcon.com, "Sensorcon - sensing products " 2016.

[3] https://www.adafruit.com/category/35, "Adafruit Industries," 2016.

[4] Webmd.com, "Asthma and Cities: Which Cities Rank Best? http://www.webmd.com/asthma/features/asthma-and-cities-which-cities-ran-best."

[5] R. M. Savola, H. Abie, and M. Sihvonen, "Towards metrics-driven adaptive security management in E-health IoT applications," in *Proceedings of the 7th International Conference on Body Area Networks*, 2012, pp. 276-281.

[6] R. M. Savola and H. Abie, "Metrics-driven security objective decomposition for an e-health application with adaptive security management," in *Proceedings of the International Workshop on Adaptive Security*, 2013, p. 6.

[7] K. Kang, Z.B. Pang, and C. Wang, "Security and privacy mechanism for health internet of things," *The Journal of China Universities of Posts and Telecommunications,* vol. 20, pp. 64-68, 2013.

[8] O. Said and A. Tolba, "SEAIoT: Scalable E-Health Architecture based on Internet of Things," *International Journal of Computer Applications,* vol. 59, pp. 44-48, 2012.

[9] J. A. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, *et al.*, "Participatory sensing," 2006.

[10] S. C. Mukhopadhyay, "Internet of Things."

[11] R. S. Istepanian, A. Sungoor, A. Faisal, and N. Philip, "Internet of M-health Things'm-IOT'," 2011.

[12] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Net. and Comp. Applications,* 2014.

[13] A. Jøsang and S. L. Presti, "Analysing the relationship between risk and trust," in *Trust Management*, ed: Springer, 2004, pp. 135-145.

[14] Z. Malik and A. Bouguettaya, "Rateweb: Reputation assessment for trust establishment among web services," *The VLDB Journal—The Int. J. on Very Large Data Bases,* vol. 18, pp. 885-911, 2009.

[15] E. Ayday and F. Fekri, "An iterative algorithm for trust management and adversary detection for delay-tolerant networks," *IEEE Transactions on Mobile Computing,* vol. 11, pp. 1514-1531, 2012.

[16] www.lantronix.com, "Improve Patient Care and Diagnostic Efficiency http://www.lantronix.com/solutions/medical.html," 2014.

[17] newscenter.verizon.com, "Verizon Gains FDA Clearance for Remote Health Monitoring Solution - See more at: http://newscenter.verizon.com/corporate/news-articles/2013/08-08-fda-clearance-for-remote-health-monitoring/#sthash.kpgSQz97.dpuf," August 8, 2013 2013.

[18] S. M. Khan and K. W. Hamlen, "Hatman: Intra-cloud trust management for Hadoop," in *Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on*, 2012, pp. 494-501.

[19] I.R. Chen, J. Guo, and F. Bao,"Trust Management for SOA-based IoT and Its Application to Service Composition," *IEEE Transactions on Service Computing*, 2016.

[20] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness Management in the Social Internet of Things," *IEEE Transactions on Knowledge and Data Management*, vol. 26, no. 5, 2014, pp. 1253-1266.

[21] Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," Computers and Security, vol. 39, Nov. 2013, pp. 351-365.